HIPAA Privacy and Security Standards: Systems Implications

Paul C. Tang, MD

Palo Alto Medical Foundation

Sutter Health

Outline

- The case for patient care and common sense
- Systems implications of key provisions of final Privacy Rule
- Systems implications of key provisions of Security NPRM

The Case for Patient Care
Principles for Using Health Information

- Patient-care decisions based on complete, accurate information; requires patient trust
- Access to individually identifiable health information based on professional need to know
- Individually identifiable information used only for purposes under which it was acquired, unless otherwise authorized for appropriate, legal reasons
- Everyone accountable for handling confidential information properly

HIPAA Mandated Standards

- HHS Secretary must adopt standards for:
  - Electronic transactions
  - Code sets
  - Unique health identifiers
  - **Privacy** and security
  - Electronic signatures

Privacy and Confidentiality

Privacy

Privacy is the individual's right to keep certain information to him or herself, with the understanding that the information will only be used or disclosed with his or her permission, or as permitted by law

Confidentiality

Confidentiality is the practice of permitting only certain authorized individuals to access information, with the understanding that they will only disclose it to other authorized individuals who have a need to know

Provider Definitions

- Direct treatment relationship – direct relationship between provider and individual
- Indirect treatment relationship – provide care under orders of another provider (e.g., radiologist, pathologist)
- Use – employment, application, utilization, examination, or analysis of information within entity
- Disclosure – release, transfer, provision of access to, divulging of information outside of entity (including disclosure to business associate)

Protected Health Information

Individually Identifiable Health Information

- "All individually identifiable health information in any form, electronic or non-electronic, that is held or transmitted by a covered entity." Includes:
  - Electronic records
  - Paper records
  - Oral communication

Rights of Patients

Access and Accountability

Individual Access to PHI
Providing Access

- Rights to summary and/or underlying information
- Act within 30 days (60 days if off-site)
- Fees for labor and supply for copying or summarizing, but not retrieving and handling information
- Fees for explanation OK
- System implication: medical record printout or electronic access via secure web server

Right to Request Amendment
To the Medical Record

- If agree, must act on request within 60 days, and:
  - Notify persons identified by individual who received PHI
  - Notify persons known to have relied on unamended information to detriment of individual
- May decline amendment if:
  - Did not create information
  - Information is accurate and complete
  - Not part of a designated record
- If denied, must inform individual of right to disagree, complain to Secretary, and include request/denial with future disclosures
- System implication: capture patient-submitted amendments

Consent Requirements
Use and Disclosure of PHI

- Health care providers with direct treatment relationship must obtain consent to use or disclose PHI for treatment, payment, or "health care operations"
- Valid indefinitely unless revoked
- Providers may condition treatment on consent
- Must inform individual of right to restrict use and disclosure, and that covered entity does not have to agree. However, agreement is binding.
- Revocable at any time, but covered for acts in reliance on prior consent
- System implication: capture patient consent and revocation

Authorizations
Use and Disclosure of PHI

- Required for all uses or disclosures not otherwise permitted for treatment, payment or health care ops
- Required for psychotherapy notes
- Required to access the medical record of another covered entity (ie., Release of Information)
- May not condition treatment on signing
- Revocable
- System implication: record of disclosure information

Authorizations
Core Elements Required

- Name of entity authorized to use or disclose
- Description of information
- Name or types of recipients
- Statement of financial remuneration, if applicable
- Expiration date or event
- Signatures
- Notice of right to revoke in writing

Accounting of Disclosures

- Right to accounting of disclosures for preceding 6 years by covered entity or its business associates for purposes other than treatment, payment, or health care operations (60 days to fulfill request)
- Accounting includes:
  - Date, name/address
  - Description of information
  - Purpose (unless requested by individual)
  - Summary of recurrent disclosures permitted
- One free accounting per 12 months
- System implication: record of disclosure information

Responsibilities and Obligations of Covered Entities

Providers

Minimum Necessary Provision
Implementing "Need-to-Know"

- Must establish policies and procedures for routine uses and disclosures and make reasonable efforts to:
  - Restrict access and use based on role
  - Limit disclosures to what is reasonably necessary for intended purpose
- Disclosures to individuals and to providers for treatment are exempt from minimum necessary rule
- Request for entire record without documented justification violates rule
- System implications: role-based access, granular audit trails

Research Uses and Disclosures

- All research covered regardless of funding
- Privacy review by IRB or privacy board for waivers
  - Minimal privacy risk
  - Waiver not adversely affect privacy rights and welfare of subjects
  - Research not practically conducted without waiver
  - Research not practically conducted without PHI
  - Research importance outweighs privacy risk
  - Adequate plan to destroy the identifiers as soon as possible (unless health or research justification)

Use of Aggregate De-identified Data *Methods*

- Apply generally accepted statistical and scientific principles to render information not identifiable
  - Document analysis and results
- Safe harbor method
  - System implication: create de-identified research database

De-Identifying Data

Safe Harbor List of Identifiers to Remove

- Name
- Address (except 3-digit zip unless <20K people)
- All dates (except year) and aggregate 90+ year olds
- Telephone numbers
- Fax numbers
- Email addresses
- Social security number
- Medical record number
- Health plan number
- Account numbers
- Certificate/license numbers
- Vehicle numbers
- Device identifiers
- URLs
- IP addresses
- Biometric identifiers
- Full-face photos
- Any other unique identifying number, characteristic, or code

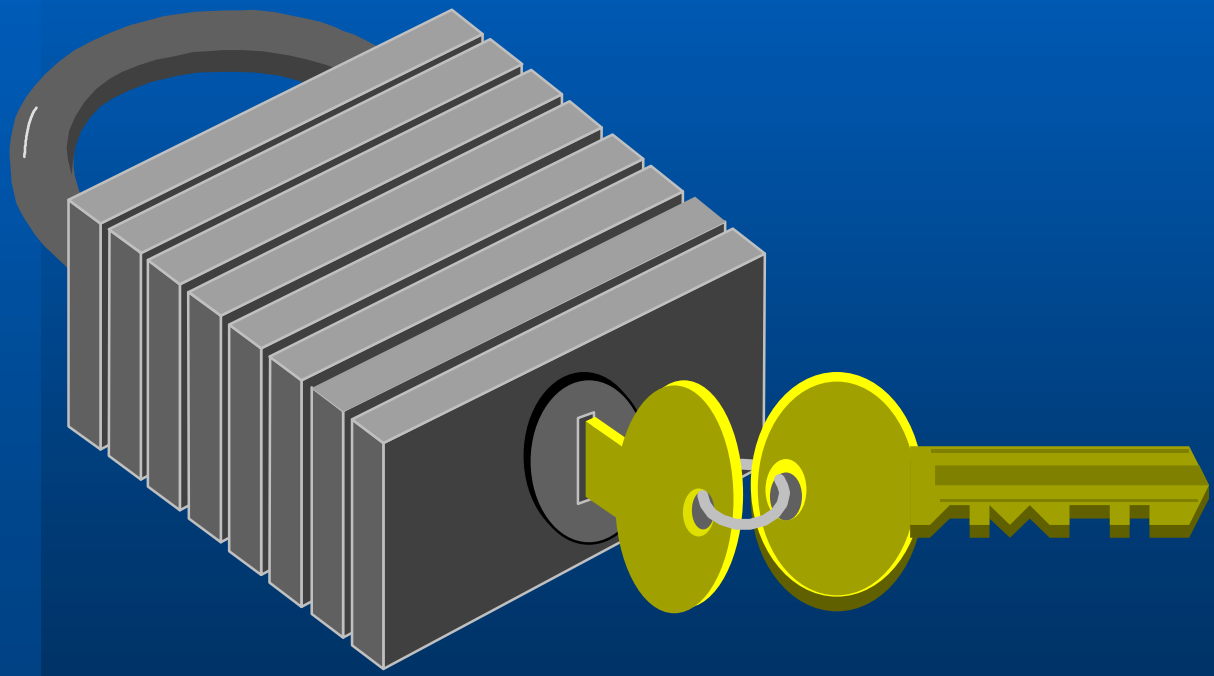
Federal Preemption of State Laws
Floor

- "More stringent" state laws are not preempted
  - Concern
    - Definition of "more stringent"
    - Inter-state nature of health care delivery
    - Complex patchwork of laws and regulations
    - May result in failure to disclose or blanket releases
  - Recommendation
    - Preemptive federal legislation

Penalties for Violating Patient Confidentiality
Civil and Criminal

- Wrongful disclosure of individually identifiable health information information
  - Civil: $100/person/violation, max $25K/person/standard/yr
  - Penalties of $50,000 to $250,000 and 1 to 10 years in jail
- Enforcement: NPRM 2001
- Responsibility of HHS Office for Civil Rights

Security



Status of Security Regulations

- Secretary issued NPRM for security regulations Aug, 98
- Secretary expected to issue regulations governing system security early 2002
- Applies to all electronic data – transmitted or stored

http://aspe.hhs.gov/admnsimp/bannerps.htm#security

Security Standards

Controlling Access, Integrity, and Disclosure

- Policy
- Physical controls
- Software controls

Security: Policies and Procedures
Establishing Guidelines and Requirements

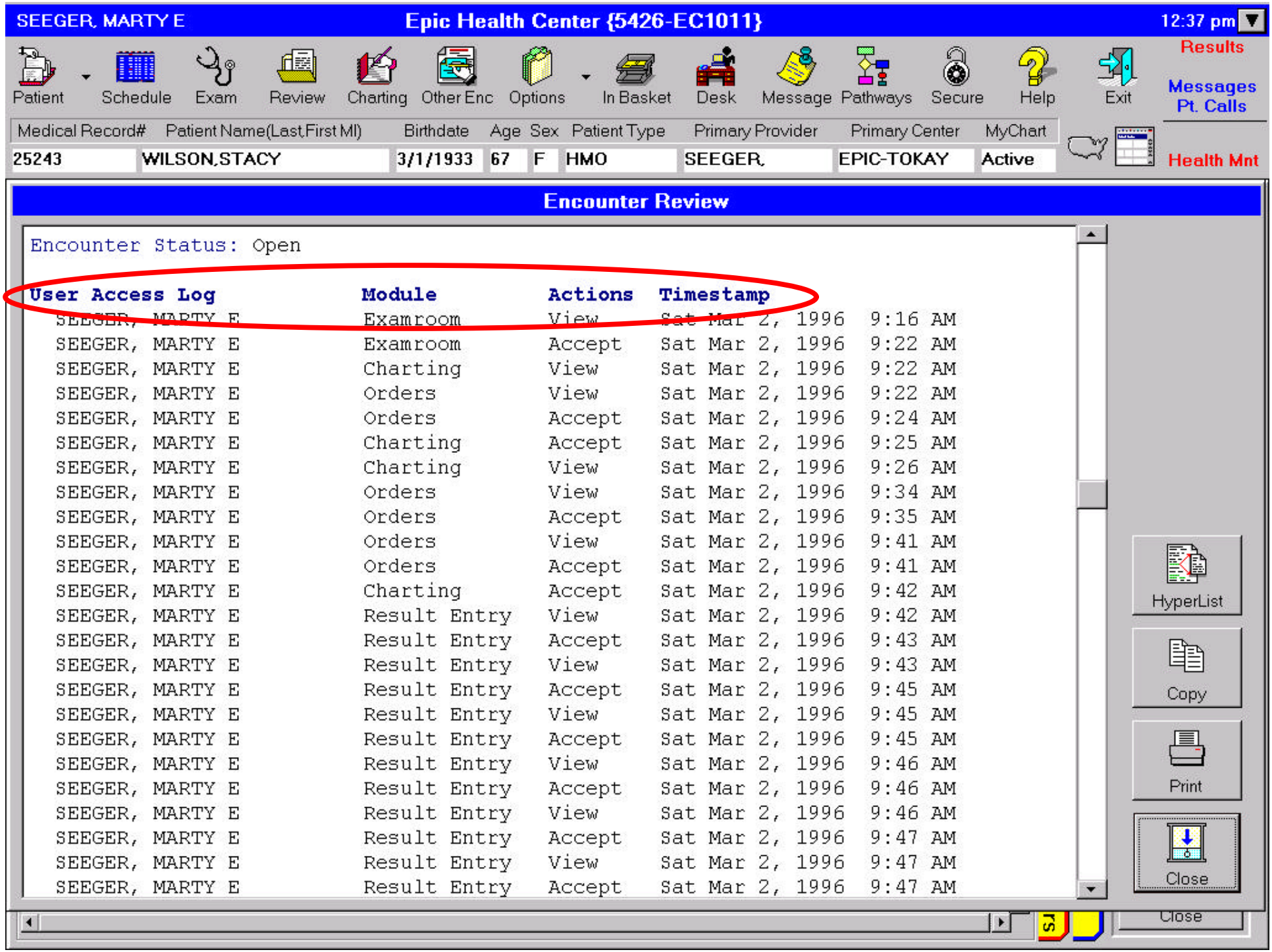
- Security officer
- Security management
- Information access policies
- User access privileges
- Annual confidentiality agreements
- Training
- Security incident procedures
- Termination procedures
- Chain of trust partner agreements
- Contingency plans
- Internal audit
- Certification of compliance

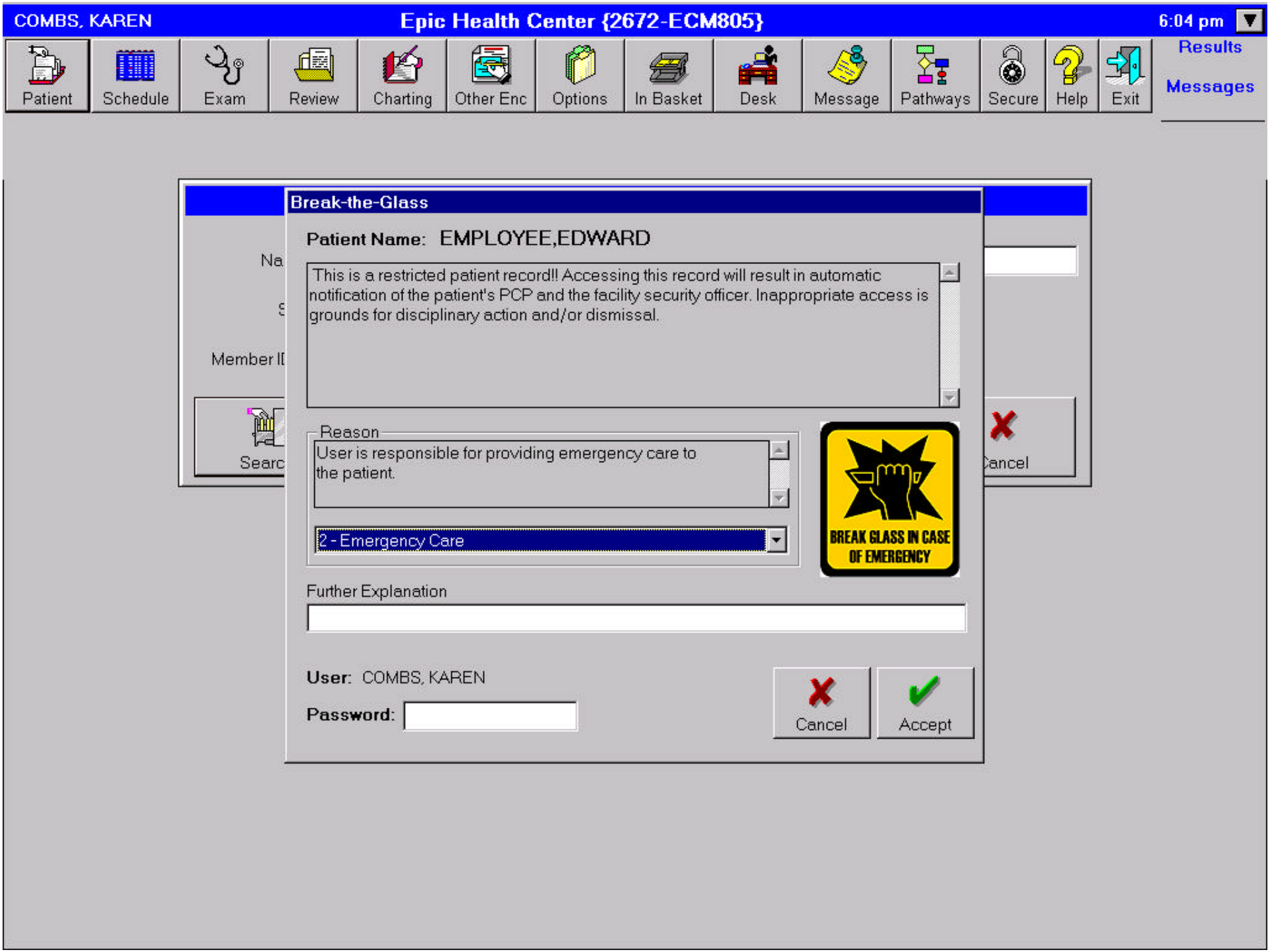
Security: Physical Controls

- Restricted access to sensitive areas
  - Data center (e.g., servers)
  - Networks (e.g., routers, network closets)
  - Workstations (e.g., public areas vs. private offices)
- Media control and disposal
- Backup systems
- Uninterruptible power supply

Security: Software Controls
System Implications

- Authorization control (e.g., who has access)
- Access privileges (e.g., what can they see)
  - Role-based, user-based accesses
  - Emergency access
- Authentication control (e.g., who they are)
- Password controls (e.g., expiration, nonrepeating, suspension)
- Audit controls
  - Retrospective
  - Warnings (e.g., break-the-glass)
- Data integrity
- Workstation timeout
- Automatic backup
- Virus protection


SEEGER, MARTY E
Epic Health Center {5426-EC1011}
12:37 pm
Patient
Schedule
Exam
Review
Charting
Other Enc
Options
In Basket
Desk
Message
Pathways
Secure
Help
Exit
Results
Messages
Pt. Calls
Health Mnt
Medical Record#
Patient Name(Last,First MI)
Birthdate
Age
Sex
Patient Type
Primary Provider
Primary Center
MyChart
25243
WILSON,STACY
3/1/1933
67
F
HMO
SEEGER,
EPIC-TOKAY
Active
Encounter Review
Encounter Status: Open
User Access Log
Module
Actions
Timestamp
SEEGER, MARTY E Examroom View Sat Mar 2, 1996 9:16 AM
SEEGER, MARTY E Examroom Accept Sat Mar 2, 1996 9:22 AM
SEEGER, MARTY E Charting View Sat Mar 2, 1996 9:22 AM
SEEGER, MARTY E Orders View Sat Mar 2, 1996 9:22 AM
SEEGER, MARTY E Orders Accept Sat Mar 2, 1996 9:24 AM
SEEGER, MARTY E Charting Accept Sat Mar 2, 1996 9:25 AM
SEEGER, MARTY E Charting View Sat Mar 2, 1996 9:26 AM
SEEGER, MARTY E Orders View Sat Mar 2, 1996 9:34 AM
SEEGER, MARTY E Orders Accept Sat Mar 2, 1996 9:35 AM
SEEGER, MARTY E Orders View Sat Mar 2, 1996 9:41 AM
SEEGER, MARTY E Orders Accept Sat Mar 2, 1996 9:41 AM
SEEGER, MARTY E Charting Accept Sat Mar 2, 1996 9:42 AM
SEEGER, MARTY E Result Entry View Sat Mar 2, 1996 9:42 AM
SEEGER, MARTY E Result Entry Accept Sat Mar 2, 1996 9:43 AM
SEEGER, MARTY E Result Entry View Sat Mar 2, 1996 9:43 AM
SEEGER, MARTY E Result Entry Accept Sat Mar 2, 1996 9:45 AM
SEEGER, MARTY E Result Entry View Sat Mar 2, 1996 9:45 AM
SEEGER, MARTY E Result Entry Accept Sat Mar 2, 1996 9:45 AM
SEEGER, MARTY E Result Entry View Sat Mar 2, 1996 9:46 AM
SEEGER, MARTY E Result Entry Accept Sat Mar 2, 1996 9:46 AM
SEEGER, MARTY E Result Entry View Sat Mar 2, 1996 9:46 AM
SEEGER, MARTY E Result Entry Accept Sat Mar 2, 1996 9:47 AM
SEEGER, MARTY E Result Entry View Sat Mar 2, 1996 9:47 AM
SEEGER, MARTY E Result Entry Accept Sat Mar 2, 1996 9:47 AM
HyperList
Copy
Print
Close
Close


COMBS, KAREN
Epic Health Center {2672-ECM805}
6:04 pm
Patient
Schedule
Exam
Review
Charting
Other Enc
Options
In Basket
Desk
Message
Pathways
Secure
Help
Exit
Results
Messages
Break-the-Glass
Patient Name: EMPLOYEE,EDWARD
This is a restricted patient record!! Accessing this record will result in automatic notification of the patient's PCP and the facility security officer. Inappropriate access is grounds for disciplinary action and/or dismissal.
Reason
User is responsible for providing emergency care to the patient.
2 - Emergency Care
BREAK GLASS IN CASE OF EMERGENCY
Further Explanation
User: COMBS, KAREN
Password:
Cancel
Accept

Summary
Do No Harm to Patient Data

- Patients first: balance goals of care with protection of information; apply common sense
- Privacy rule mostly policies and behaviors
- System security must facilitate implementation and enforcement of privacy policies (e.g., minimum necessary, disclosure record)